## AMENDMENTS TO THE SPECIFICATION

*Please replace paragraph [0004] on page 3 with the following rewritten paragraph.*

[0004] In the public key infrastructure (PKI), certificate authorities are organized in a hierarchical structure. Certificate authorities at the highest level ~~is~~ are called root certificate authorities. A series of certificates are signed by a series of certificate authorities up to the root certificate authority in a hierarchical order. A certificate of a certificate authority is used for verification of the public key of a subordinate certificate authority in the hierarchical order. Thus, for the verification of a certificate, a chain of certificates or an entire list up to the root certificate authority has to be acquired.

*Please replace paragraph [0005] spanning pages 3 and 4 with the following rewritten paragraph.*

[0005] Recently, secure encrypted communication such as Secure Sockets Layer (SSL) communication is needed in a network environment. SSL is a communication protocol for transmitting encrypted data between a web server and a web browser, wherein public key encryption and electronic certificates are used to send data securely. For secure data communication with use of SSL protocol or the like, a server apparatus which sends data needs a certificate. A certificate can be purchased from an external certificate authority which gives a service to issue a certificate. However, in a network such as an intranet, a user would not want to buy an expensive certificate from an authority outside the network only for SSL communication. On the other hand, a certificate may be created by a server apparatus. However, when a certificate created by the server apparatus is used, because the certificate is not issued by a certificate authority, a warning is given in a warning dialog in the screen of the server apparatus to inform the user ~~of that~~ that the certificate is not trusted. This is because a list of certificates up to the root certificate authority is not available.

*Please replace paragraph [0007] spanning pages 4 and 5 with the following rewritten paragraph.*

In one aspect of the invention of a communication system wherein a device and a client communicate with each other through a network, the device comprises a first storage device which stores a root certificate including a public key ~~in a pair of the public key and~~ paired with a private key and being signed with the ~~public~~ private key, a certificate creator which creates a second certificate including the root certificate designated as a certificate authority at high level and signed with the private key, and a communication device which transmits the second certificate created by said certificate creator. The client comprises a second storage device which stores the root certificate stored in said first storage device, and a verifier which verifies the signature of the second certificate received from said device with the public key.

*Please replace the paragraph beginning at line 11 on page 5 with the following rewritten paragraph.*

In another aspect of the invention of a device to be used in a communication system between the device and a client through a network wherein the device sends information to a client and the client uses the information to communicate with the device, the device comprises a first storage device which stores a pair of a public key and a private key, a second storage device which stores a root certificate signed with the ~~public~~ private key, and an interface which sends the information as well as the public key to the client through the network. The root certificate is sent through said interface to the client for verification of the information by the client.

*Please replace paragraph [0022] spanning pages 7 and 8 with the following rewritten paragraph.*

[0022] Referring now to the drawings, wherein like reference characters designate like or corresponding parts throughout the several views, Fig. 1 shows a data communication system for communicating data through a network. A device 100 such as a printer or a multifunctional peripheral (MFP) and a client 200 such as a personal computer are connected to a network 300 such as an intranet or a local area network.

In the network 300, Secure Sockets Layer (SSL) is used as a communication protocol. The device is operated as a server for the client 200, and it has a web server 120 which supports SSL. The client 200 is, for example, a personal computer (PC) and has a web browser (also referred ~~also~~ to as a browser) 216 which supports SSL. The web server 120 of the device 100 and the browser 216 of the client 200 can transmit data between each other by using SSL. Though only one device 100 and only one client 200 are shown in Fig. 1, a plurality of devices 100 and a plurality of clients 200 can be connected to the network 300 generally.

*Please replace paragraph [0023] on page 8 with the following rewritten paragraph.*

[0023] Fig. 2 shows an internal structure of a multifunctional peripheral as an example of the device 100. The multifunctional peripheral has a scanner 102 for reading a document image, a print engine 104 for printing an image, a communication device 106 for ~~communication~~ communicating through the network 300, and an operation panel 108 for receiving a user's instruction of an operation and for display. Further, a central processing unit (CPU) 110 is connected through an internal bus 112 to a random access memory (RAM) 114, a read-only memory (ROM) 116, a storage device 118 such as a hard disk drive, a scanner controller 132 and a print controller 134 as well as the above-mentioned components 102-108. The scanner controller 132 controls the scanner 102, and the print controller 134 controls the print engine 104. The multifunctional peripheral serves as a printer, a copying machine, a scanner and the like. The storage device 118 stores programs such as the web server 120 supporting SSL, a program 122 for creating a root certificate, and a program 124 for creating a self-made certificate, and data such as a root certificate 126, a self-made certificate 128 and files 130.

*Please replace paragraph [0024] spanning pages 8 and 9 with the following rewritten paragraph.*

[0024] Fig. 3 shows an internal structure of a personal computer as an example of the client 200. The personal computer has a central processing unit (CPU) 202 which controls the entire system, and a random access memory (RAM) 114 and a

read-only memory (ROM) 116 both connected to the CPU 202. The CPU 202 is further connected to a display device 208, input devices 210 such as a keyboard and a mouse, and a communication device 212 for ~~communication~~ communicating through the network 300. The CPU 202 is also connected to a hard disk drive (HDD) 214 for storing programs and data, and a CD drive 226 for access with a compact disk (CD) 226a. A storage device such as the hard disk or the compact disc stores programs such as an operating system (not shown), the web browser 216 supporting SSL, a printer driver 218, and a program 220 for installing a root certificate to the client 200, and data such as a root certificate 222, and files 224 to be transmitted. The printer driver 218 generates print data to be sent to a printer or multifunctional peripheral as one of the devices 100.

*Please replace paragraph [0026] spanning pages 9 to 11 with the following rewritten paragraph.*

[0026] When the web server 120 in the device 100 and the web browser 216 in the client 200 transmit data between ~~them~~ themselves in SSL protocol, the device (or server) is verified, the client is verified, and the contents of communication ~~is~~ are encrypted. The device 100 holds the root certificate ~~122~~126. The root certificate ~~122~~ 126 may be created by the device 100 itself or issued by a certificate authority (CA). In this embodiment, it is created by the device 100, as will be explained later. When the root certificate is created by the device 100, it is an advantage that the attributes of the root certificate can be changed freely by the device 100. The root certificate ~~122~~ 126 includes a public key created when the root certificate is created. On the other hand, the root certificate ~~122~~ 126 has also been installed in the client 200 beforehand. This is the above-mentioned root certificate ~~220~~ 222 stored in the client 200. The installation of a root certificate is preferably performed automatically. For example, it is installed when the printer driver 218 for the device 100 is installed in the client 200. Preferably, before the root certificate is installed, it is requested for a user to approve the installation. Because the client 200 holds the root certificate ~~220~~222, a certificate issued by a certificate authority outside the network 300 is not needed to verify the certificate received from the device 100, as will be explained

later. If a storage device such as ROM 206 storing the root certificate ~~220~~ 222 is supplied to the client 200, forgery of the root certificate is prevented.

*Please replace paragraph [0036] on page 14 with the following rewritten paragraph.*

[0036] D) Next, the two hash values obtained above are compared with each other to confirm that they are the same. If the two values are the same, it is verified that the self-made certificate is not tampered with.

*Please replace paragraph [0039] spanning pages 15 and 16 with the following rewritten paragraph.*

[0039] Fig. 9 shows a flowchart of the verification of a certificate sent from the device (server) 100 executed by the CPU 202 of the client 200. This is a part only on a root certificate for the verification with SSL protocol in the browser 216. The verification is started when a certificate is received from the device (server) 100. First, a certificate at the high level (the root certificate in this example) is acquired based on the information in the certificate (S40), and it is decided whether or not the certificate authority (CA) at the higher level can be trusted (S42). If the certificate authority is registered as a trusted root certificate in the client 200, or if it is asked to verify the root certificate through the Internet to find that it is registered as a trusted root certificate, the certificate authority is decided to be trusted. In this example, because the root certificate has been installed beforehand and is registered as a trusted certificate authority, it is decided that the certificate authority at the higher level is trusted. Because the certificate authority at the higher level is trusted, the signature is decrypted with the public key of the root certificate (S44). If the decryption is completed (YES at S46), it is decided that the certificate is verified by the certificate authority at the higher level.

*Please replace paragraph [0041] on page 17 with the following rewritten paragraph.*

[0041] On the other hand, if the certificate authority at the higher level is not trusted, or if the signature cannot be decrypted, or if the two hash values, Hash1 and

Hash2, are not the same, the certificate is decided not to be trusted. Then, a warning is displayed in the screen of the display device to inform the user ~~of that~~ that the certificate is not trusted (S54).

*Please replace paragraph [0048] spanning pages 19 to 21 with the following rewritten paragraph.*

[0048] In an example shown in Fig. 12, a certificate chain has three hierarchical levels of a root certificate, an intermediate certificate and a self-made certificate. The device 100 such as a printer or a multifunctional peripheral holds the root certificate and the intermediate certificate and has installed them beforehand to the client 200. In SSL transmission, the device 100 creates a pair of a public key and a private key, and creates a self-made certificate including the public key. The intermediate certificate designates the root certificate as a certificate authority at a higher level and adds the sign to the certificate, and the self-made certificate designates the intermediate certificate as a certificate authority at a higher level and incorporates the sign to the certificate. The device 100 obtains a hash value by using a predetermined hash function on the self-made certificate including the intermediate certificate as a certificate authority at a higher level, performs signature and adds it to the self-made certificate. Then the data and the self-made certificate are transmitted to the client 200. When the client 200 verifies the transmitted self-made certificate, it uses a chain of certificates which have been installed. Because the self-made certificate designates the intermediate certificate as the certificate of a certificate authority at a higher level, the verification of the self-made certificate is performed by using the installed intermediate certificate. Further, the intermediate certificate is verified by using the root certificate already installed. Thus, the self-made certificate is decided to be a trusted certificate.